Training Course on Custom Threat Hunting Queries (Splunk, ELK)

Professional Development Training Course Outline

Category	Digital Forensics	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today's dynamic cyber threat landscape, traditional security defenses are often insufficient to detect sophisticated and **advanced persistent threats (APTs)**. Organizations require proactive **threat hunting** capabilities to identify hidden adversaries and **zero-day exploits** before significant damage occurs. Training Course on Custom Threat Hunting Queries (Splunk, ELK) empowers cybersecurity professionals with the essential skills to develop and implement custom threat hunting queries using industry-leading **Security Information and Event Management (SIEM)** platforms, specifically **Splunk** and the **ELK Stack (Elasticsearch, Logstash, Kibana)**. Participants will learn to leverage the power of **big data analytics** and **behavioral anomaly detection** to proactively uncover malicious activities, significantly enhancing their organization's **cyber resilience** and **incident response** capabilities.

This practical, hands-on program delves deep into **log analysis**, **data correlation**, and the creation of targeted **detection rules**. Through real-world **case studies** and interactive exercises, attendees will master the art of transforming raw security data into actionable **threat intelligence**. By focusing on both Splunk's powerful **SPL (Search Processing Language)** and ELK's flexible **Kibana Query Language (KQL)**, this course ensures comprehensive coverage, preparing security analysts to effectively hunt for emerging threats across diverse IT environments. This **advanced cybersecurity training** is crucial for maintaining a robust **security posture** in the face of evolving **cyber attacks**.

Programme Curriculum

Training Course on Custom Threat Hunting Queries (Splunk, ELK)

Introduction

In today's dynamic cyber threat landscape, traditional security defenses are often insufficient to detect sophisticated and **advanced persistent threats (APTs)**. Organizations require proactive **threat hunting** capabilities to identify hidden adversaries and **zero-day exploits** before significant damage occurs. Training Course on Custom Threat Hunting Queries (Splunk, ELK) empowers cybersecurity professionals with the essential skills to develop and implement custom threat hunting queries using industry-leading **Security Information and Event Management (SIEM)** platforms, specifically **Splunk** and the **ELK Stack (Elasticsearch, Logstash, Kibana)**. Participants will learn to leverage the power of **big data analytics** and **behavioral anomaly detection** to proactively uncover malicious activities, significantly enhancing their organization's **cyber resilience** and **incident response** capabilities.

This practical, hands-on program delves deep into **log analysis**, **data correlation**, and the creation of targeted **detection rules**. Through real-world **case studies** and interactive exercises, attendees will master the art of transforming raw security data into actionable **threat intelligence**. By focusing on both Splunk's powerful **SPL (Search Processing Language)** and ELK's flexible **Kibana Query Language (KQL)**, this course ensures comprehensive coverage, preparing security analysts to effectively hunt for emerging threats across diverse IT environments. This **advanced cybersecurity training** is crucial for maintaining a robust **security posture** in the face of evolving **cyber attacks**.

Course Duration

10 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Proficiently analyze vast volumes of security logs from diverse sources.
2. Craft sophisticated SPL queries for effective threat hunting and **anomaly detection**.
3. Leverage Elasticsearch, Logstash, and Kibana for **threat intelligence** and investigative analysis.
4. Identify unusual user and system behaviors indicative of compromise.
5. Map observed adversary tactics, techniques, and procedures (TTPs) to real-world attacks.
6. Design and implement effective alerts and correlation rules in Splunk and ELK.
7. Script and automate repetitive hunting tasks for increased efficiency.
8. Incorporate external threat data for enriched context and proactive hunting.
9. Understand basic static and dynamic analysis techniques to inform query development.
10. Analyze network traffic and flow data for suspicious patterns and C2 communications.
11. Develop queries to detect malicious or unintentional insider activities.
12. Understand best practices for efficient data ingestion and query optimization in Splunk and ELK.
13. Effectively communicate findings and recommendations to stakeholders.

Organizational Benefits

- Identify and neutralize cyber threats *before* they escalate into major breaches, minimizing **dwell time**.
- Streamline investigations and accelerate remediation efforts, reducing **business disruption**.
- Proactively discover vulnerabilities and blind spots in existing defenses, improving overall **cyber resilience**.
- Prevent costly data breaches, regulatory fines, and reputational damage.

- Generate internal threat intelligence based on observed adversary behaviors, fostering a more **proactive security** approach.
- Maximize the value of existing Splunk and ELK stack deployments through expert-level utilization.
- Cultivate a highly competent and specialized **cybersecurity workforce** capable of tackling sophisticated threats.
- Bolster compliance with industry regulations by demonstrating robust **threat detection** and **data protection** capabilities.

Target Audience

1. Security Analysts (Tier 2/3)
2. Threat Hunters
3. SOC Analysts
4. Incident Responders
5. Security Engineers
6. Forensics Investigators
7. Security Architects
8. IT Security Managers

Course Outline

Module 1: Introduction to Threat Hunting & Methodologies

- Define proactive threat hunting vs. reactive security.
- Explore common threat hunting methodologies (hypothesis-driven, intelligence-driven, anomaly-driven).
- Understand the threat hunting loop and its iterative nature.
- Discuss the importance of data sources and visibility for successful hunts.
- Case Study: Analyzing a persistent threat actor's initial access techniques to formulate a hunting hypothesis.

Module 2: Splunk Fundamentals for Threat Hunting

- Review Splunk architecture, data ingestion, and indexing.
- Master basic and advanced Splunk Search Processing Language (SPL) commands.
- Utilize Splunk data models and pivot tables for efficient analysis.
- Understand Splunk fields, extractions, and knowledge objects.
- Case Study: Using Splunk to identify unusual login patterns after an initial alert.

Module 3: ELK Stack Fundamentals for Threat Hunting

- Overview of Elasticsearch, Logstash, and Kibana architecture.
- Data ingestion with Logstash and Beats (Filebeat, Winlogbeat, Packetbeat).
- Kibana interface navigation, dashboards, and visualizations.
- Mastering Kibana Query Language (KQL) for efficient searching.
- Case Study: Ingesting Windows Event Logs into ELK to search for specific security events.

Module 4: Data Sources & Log Management for Hunting

- Identify critical data sources for threat hunting (endpoint, network, cloud, authentication).
- Strategies for centralized log collection and normalization.
- Understanding log formats and parsing challenges.

- Best practices for data retention and storage optimization.
- Case Study: Correlating firewall logs with web server logs to detect web shell activity.

Module 5: Hypothesis-Driven Threat Hunting

- Developing strong threat hunting hypotheses based on threat intelligence or observed anomalies.
- Translating hypotheses into actionable Splunk and ELK queries.
- Refining hypotheses based on initial hunt results.
- Documenting hunt progress and findings.
- Case Study: Hypothesis: "An attacker is using PowerShell for fileless malware execution." Developing queries to test this.

Module 6: Intelligence-Driven Threat Hunting

- Integrating external threat intelligence feeds (STIX/TAXII, OSINT).
- Leveraging **Indicators of Compromise (IOCs)** and **Indicators of Attack (IOAs)**.
- Mapping threat intelligence to MITRE ATT&CK TTPs.
- Creating watchlists and lookups for automated detection.
- Case Study: Using CISA alerts for a newly discovered vulnerability to hunt for exploitation attempts.

Module 7: Anomaly-Driven Threat Hunting

- Understanding baselines and normal network/user behavior.
- Techniques for identifying statistical outliers and deviations.
- Leveraging Splunk's anomalydetection and ELK's machine learning capabilities.
- Dealing with false positives and refining anomaly detection models.
- Case Study: Detecting unusual data exfiltration volumes or off-hour access patterns.

Module 8: Hunting for Endpoint Compromises

- Endpoint telemetry sources (Sysmon, EDR, endpoint logs).
- Hunting for malicious process execution and DLL sideloading.
- Detecting persistence mechanisms (registry run keys, scheduled tasks).
- Analyzing file system changes and suspicious file creations.
- Case Study: Identifying lateral movement attempts using suspicious PsExec or WMI activity.

Module 9: Hunting for Network Intrusions

- Analyzing network flow data (NetFlow, IPFIX) for unusual connections.
- Deep packet inspection (DPI) and protocol analysis.
- Detecting C2 communications and beaconing activity.
- Hunting for port scanning, brute-force attempts, and network reconnaissance.
- Case Study: Discovering hidden tunnels or exfiltration over non-standard ports.

Module 10: Hunting in Cloud Environments

- Understanding cloud log sources (AWS CloudTrail, Azure Activity Logs, GCP Audit Logs).
- Hunting for suspicious API calls and cloud resource modifications.
- Detecting unauthorized access to cloud storage and services.
- Identifying misconfigurations that could lead to compromise.
- Case Study: Hunting for privilege escalation or unusual EC2 instance launches in AWS.

Module 11: Insider Threat Hunting

- Indicators of insider threat (data exfiltration, privilege abuse, policy violations).
- Monitoring user activity, data access, and unusual application usage.
- Techniques for correlating user identity with suspicious actions.
- Developing behavioral profiles for insider risk assessment.
- Case Study: Detecting an employee downloading sensitive data to a personal device just before resignation.

Module 12: Advanced Splunk Threat Hunting Techniques

- Using subsearches and macros for complex query construction.
- Leveraging Splunk Enterprise Security (ES) for integrated hunting.
- Developing custom correlation searches and risk-based alerting (RBA).
- Splunk SOAR integration for automated response workflows.
- Case Study: Building a complex correlation search in Splunk ES to detect multi-stage attacks.

Module 13: Advanced ELK Stack Threat Hunting Techniques

- Advanced Kibana visualizations for threat hunting (Timelion, Maps, Graph).
- Using Elasticsearch queries (DSL) for precise data retrieval.
- Implementing Elastic Security rules and endpoint integrations.
- Automating hunting with Watcher and Alerting.
- Case Study: Utilizing Elastic Common Schema (ECS) to build a unified view for cross-source threat hunting.

Module 14: Reporting, Documentation & Collaboration

- Effective communication of threat hunting findings to technical and non-technical audiences.
- Creating detailed hunt reports and playbooks.
- Establishing a feedback loop for continuous improvement of hunting efforts.
- Collaboration strategies within the SOC and with other security teams.
- Case Study: Presenting findings of a successful hunt for a novel ransomware variant and recommending new detection rules.

Module 15: Building a Threat Hunting Program

- Defining roles and responsibilities within a threat hunting team.
- Establishing key performance indicators (KPIs) for hunting effectiveness.
- Integrating threat hunting into the overall security operations lifecycle.
- Tools and resources for continuous learning and skill development.
- Case Study: Developing a roadmap for integrating a new threat hunting capability into an existing SOC.

Training Methodology

This training course employs a highly **interactive and hands-on** methodology, ensuring practical skill development and immediate applicability. The approach includes:

- **Instructor-Led Sessions**.
- **Hands-on Labs**
- **Case Study Analysis**
- **Group Discussions & Collaboration**
- **Quiz & Assessments**.

- **Best Practices & Industry Standards**
- **Customized Exercises**.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

Start Date	End Date	Location	Price
05 Oct 2026	16 Oct 2026	Physical	$3,000
12 Oct 2026	23 Oct 2026	Physical	$3,000
19 Oct 2026	30 Oct 2026	Physical	$3,000
26 Oct 2026	06 Nov 2026	Physical	$3,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com